

DEVICE FOR SELECTIVELY BLOCKING  
REMOTE PURCHASE REQUESTS

RELATED APPLICATIONS

5         This application is a divisional of application serial no. 09/513,608, filed February 25, 2000, which is a divisional of application serial no. 09/017,403, filed February 2, 1998, which is now U. S. Patent Number 6,108,642 issued on August 22, 2000.

10

BACKGROUND OF THE INVENTION

Merchants who sell goods on credit over the telephone or the internet ("remote sale merchants") encounter the difficult problem of credit card fraud.

15         Unlike a merchant selling goods on credit in the physical presence of the purchasers, a remote sale merchant does not have an opportunity to inspect the signature of the purchaser or to compare a photo ID card with the purchaser's actual appearance.

20         Typically, a remote sale merchant employs a computer system having terminals or "voice response units," each of which is connected with a telephone line and is controlled by an operator wearing the commonly familiar telephone headset and receiving telephone calls. Each 25 operator typically answers the telephone and receives purchase request information from the caller that includes the merchandise that the caller wishes to purchase, the person and address to which the merchandise should be delivered, the name of the person making the purchase and a 30 credit or debit card number to which the purchase should be charged. (As used in this application the term "card number" refers to any charge authorizing number including

debit card numbers, credit card numbers, or a charge authorizing number that is not shown on any card.) The operator enters this information into the terminal and presses a keyboard button which causes the computer system 5 to send an authorization query to the card issuing financial institution. The decision to authorize is typically based on whether the number is legitimate, adequate funds are available in the account, and the card holder is current on his or her payments. If the card 10 issuing financial institution declines the charge, the caller is told that the purchase cannot be made. If the financial institution accepts, a charge to the card number account is initiated and the purchase and shipping address information is automatically forwarded to the shipping 15 department which fills the order. Optionally, the financial institution may offer an address verification service (AVS). To utilize this service the remote purchase merchant transmits the shipping address or zip code to the financial institution, which responds with a flag 20 indicating whether or not the address and/or zip code matches the billing address on file.

Another computer system for effecting remote purchases is a computer system for enabling parties to purchase items over the internet or from a computer 25 connected by modem to the computer system. In such a computer system, the party making a purchase request enters his or her credit card number and a descriptor or descriptors of the merchandise to be purchased into a remote terminal that is connected by way of the internet or 30 a telephone line to the computer system. Again, the

computer system generates an authorization query to the card issuing financial institution and contacts the shipping department to fill the order if the purchase is authorized.

5           Unfortunately, there is sometimes a considerable time interval between the time a credit card is stolen and the time when the theft of the card is reported to the card issuing financial institution. Moreover, the notation and illicit use of a credit card number by a dishonest store  
10          clerk or other person able to observe the number is likely to be completely undetected until the number is used fraudulently and the card holder receives his or her statement.

When a cardholder does receive a statement  
15          bearing fraudulent charges, he or she is likely to quickly disavow the purchases. In these cases the card issuing financial institution typically will ask the merchant to corroborate the purchase with a copy of a signed credit card receipt. For the case of a remote purchase, the  
20          merchant will not be able to produce a signed receipt. In this situation the merchant is forced to accept a "charge back" and to return the funds to the card issuing institution.

Credit card fraud varies from casual fraud by the  
25          occasionally dishonest and adventurous to sophisticated operations that attempt to purchase a large quantity of a particular item and to profitably reintroduce it into the stream of commerce. As systems for selling items over the internet and telephone lines become increasingly automatic,  
30          fraud systems also become more automatic. For example, it

has been known for thieves to use a computer to invent credit card numbers and submit a large number of purchase requests, knowing that a portion of the invented card numbers will be for issued credit cards and hoping that 5 some of the purchase requests will be accepted.

Despite the occurrence of fraud, the convenience and speed of using credit cards to make remote purchases is causing a continued expansion in catalog sales, advertised telephone sales and sales over the internet.

10

#### SUMMARY OF THE INVENTION

The present invention is a method for partially verifying the legitimacy of a remote purchase request based on a card number from a card issuing financial institution. 15 The method includes receiving and storing a first purchase request information set including an origin and a card number. Further, the origin and the card number are sent to the card issuing financial institution to determine if the origin matches an origin on file for the card number at 20 the card issuing financial institution.

The foregoing and other objectives, features, and advantages of the invention will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying 25 drawings.

#### BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

FIG. 1 is a block diagram of a remote purchase processing computer system according to the present 30 invention.

FIG. 2A is a flow chart of the beginning part of the logic process implemented in the system of FIG. 1.

FIG. 2B is a flow chart of the end part of the logic process implemented in the system of FIG. 1.

5

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A preferred embodiment of the present invention comprises a remote purchase processing computer system 10 that is connected to a data line 12, over which it receives 10 a remote purchase request initiating signal (block 110 in FIG. 2a). In one preferred embodiment, data line 12 is a telephone line. In this instance, the purchase request initiating signal (block 110) would be a ring signal received over the telephone line. A data input subsystem 14 answers the ring signal, in a manner familiar to those skilled in the art of telephony, and automatically receives 15 a caller ID signal describing the telephone number of the calling station (block 112). In many systems 10, data input subsystem 14 includes a human operator or operators 20 who query the callers, hear the purchase request information (block 112) and translate the auditory purchase request information into a set of keystrokes (block 114) that are input into system 10 via a terminal keyboard. It is becoming increasingly common, however, to avoid the 25 necessity of employing a human operator by allowing the caller to enter all of the information by way of a telephone keypad. A dual tone modulated frequency translation system is used to translate information (block 114) that the purchase requestor inputs into the telephone 30 keypad. For those who are calling by way of their own

computer/modem system, data input system 14 would include a modem for collecting all of the purchase information set.

Alternatively, data line 12 could be a direct connection to the internet or some other computer network.

- 5 In this embodiment, computer system 10 receives the internet address of the purchase request information over data line 12 and subsystem 14 does not employ a human operator.

In any one of the embodiments, each assembled purchase request information set is sent (block 115) to a logic subsystem 20. Logic subsystem 20 compares the purchase request information set to information stored in a memory subsystem 22. The bulk of the information in memory subsystem 22 typically will have been gathered from previous purchase requests. Even if there are many terminals in data input subsystem 14 all of the information sets are cataloged together in memory subsystem 22 so that a more effective data bank is constructed. Information in memory subsystem 22, however, may also have been gathered from other sources. For example, a merchant may decide to not authorize purchase requests from telephone calls originating from jails and prisons. Therefore, all of the telephone numbers for telephones in jails and prisons are kept in a "negative file" of origins that will result in automatic rejection when detected (decision box 116 of FIG. 2A). Optionally, when the remote merchant determines that an origin has generated a fraudulent purchase, the fraudulent purchase generating origin is also entered into the negative file (typically this is done manually by a keyboard operator).

In one preferred embodiment, "history factors" are computed for both card numbers and origins so that the algorithm can take into account the legitimate purchase history of both the purchase request origin and card number. A purchase request from an origin or card number that has been used to make legitimate purchases from the merchant in the past is less likely to be fraudulent than a call from a origin or card number encountered for the first time. Although it is possible that a thief who has just acquired a stolen card number will make a remote purchase request to a merchant that the legitimate card holder purchased from in the past, it is more likely that the thief will have different tastes and seek to purchase from different merchants to whom the stolen card number and the thief's origin will be new. Equations 1, 2 and 3 given below show the calculation of these factors. For residences:

$$OHF = P + 0.001 \times \sum (D \times \text{Min}[N, 10]) \quad (1)$$

where OHF = origin history factor,

D = dollar purchase amount,

N = number of months since date of purchase, and

P = all same origin no fraud indication purchases more than

1 month old.

Public and semi-public telephone, OHF = 0.2 (2)

$$CNHF = P + 0.001 \times \sum (D \times \text{Min}[N, 10]) \quad (3)$$

where CNHF = card number history factor,

D = dollar purchase amount,

N = number of months since date of purchase, and

5 purchase request history factor = Max(CNHF, OHF)

P = all the same card number no fraud indication  
purchases more than

10 1 month old.

The history factors are used to determine the amount of purchases which are allowed over a particular time period as shown in decision boxes 118, 120 and 122 in FIG. 2B.

15 The longer a purchase is outstanding without being detected as fraudulent, the greater the probability that the purchase was, indeed, legitimate. For the first one month period, of course, little confidence can be had in the purchase, because there is no guarantee that the card  
20 holder has been billed for the purchase. Therefore, purchases less than one month old are not counted. After that the purchases are given greater weight as they age, until at ten months, when there is little chance of undetected fraud yet being detected, they reach their  
25 maximum weight.

Purchase requests from public and semi-public telephone numbers such as numbers originating from motels and pay telephones are given an origin history factor of 0.2, because no meaningful history can be compiled  
30 (equation 2). Also, a person wishing to commit remote purchase fraud is likely to use a telephone which cannot be traced to his or her home address, where he or she is more likely to be identified. Therefore, telephone calls

originating from public or semi-public telephones are more likely to originate fraudulent calls.

Next, an inquiry is made into whether or not an item in the same merchant-defined merchandise category has 5 been purchased within the previous merchant set time period divided by the purchase request history factor (decision box 118). Sophisticated remote purchase thieves may try to steal a sizable quantity of a particular product because it is easier to illicitly reintroduce a set of uniform items 10 back into the stream of commerce than to do the same for an eclectic mix. For example, a ring of thieves may attempt to steal 1,000 handbags of a particular popular make. By having a safeguard such as that in block 118 the merchant limits its exposure to repetitive theft from the same 15 merchandise category.

Decision boxes 120 and 122 place limits on the monetary value of a days purchase and a weeks purchase from the same origin. This enables a merchant to limit its exposure to fraud. In particular, this addresses the case 20 in which a thief has compiled a quantity of credit card numbers and is calling from the same origin, but using a different card number each time to avoid any limits placed on each card number. If a merchant prefers, time periods other than a day or a week may be chosen.

25 If the test results of decision boxes 118, 120 or 122 are positive, then the purchase is automatically blocked (block 124) and the case of an operator controlled terminal, the key which causes a query to be sent to a financial institution is disabled. Together, boxes 118, 30 120 and 122 comprise a set of criteria, any criterion of

which could cause the purchase request to be blocked, if satisfied in the negative. The term "set of criteria," as used in this application, may include as few as one criterion only.

5           If the purchase is tentatively authorized in decision box 122, the origin, card number and purchase amount, and other data as required are sent to the card issuing financial institution for verification (block 126). If the financial institution has no origin verification 10 service, then the sending of the origin may be omitted. The financial institution that does have an origin verification service will send back a signal indicating whether or not the origin matches any origin that it has on file for that card number. If any of the tests of boxes 15 118, 120 or 122 were "near misses," for example if the time since the last purchase of the same category of merchandise (box 118) was not much greater than the (user set time period)/(purchase request history factor), then a bit would be set that would cause the purchase request to be denied 20 if the origin verification was returned in the negative. The user may be queried to supply his home telephone number, so that the origin sent to the card issuing financial institution for verification will more likely be the one on file.

25           The terms and expressions which have been employed in the foregoing specification are used therein as terms of description and not of limitation, and there is no intention, in the use of such terms and expressions, of excluding equivalents of the features shown and described 30 or portions thereof, it being recognized that the scope of

the invention is defined and limited only by the claims which follow.